(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 276 937 A1**

(12) EUROPEAN PATENT APPLICATION

(21) Application number: 88300375.8

(22) Date of filing: 18.01.88

(51) Int. Cl.[4]: G 05 B 19/04

(30) Priority: 29.01.87 GB 8701964

(43) Date of publication of application:
03.08.88 Bulletin 88/31

(84) Designated Contracting States: BE DE FR IT NL

(71) Applicant: British Gas plc
Rivermill House 152 Grosvenor Road
London SW1V 3JL (GB)

(72) Inventor: Price, Barry Leonard
6 Whiteside Close Knowle
Solihull West Midlands B93 9PD (GB)

Thornhill, Christopher John
39 Mitford Drive Damsonwood
Solihull West Midlands B92 9PE (GB)

(74) Representative: Morgan, David James
British Gas plc Patents, Licensing & Commercial Dev.
326 High Holborn
London WC1V 7PT (GB)

(54) Safety monitor.

(57) A monitor system for safety critical situations such as burner control receives at inputs 17-21 control information from a programmable logic control and reference information at inputs 12-16 from plant interlocks. This information passes via opto-isolators 40 and buffers 41 to the address bus of an EPROM so as to access information stored therein which normally mirrors the PLC information so as to control relays RL1-5 via drivers 45 to conform to the PLC instructions. The EPROM also contains reset and clock information for use by a counter 48 which allows different areas within the EPROM to be accessed. The reset information is also available to a parity check circuit 49 via oscillator 46 for dynamically testing the monitor for integrity of operation. Failure of the PLC or monitor components will cause access to shutdown addresses of the EPROM and operation of the appropriate relays including lockout relay RL6.

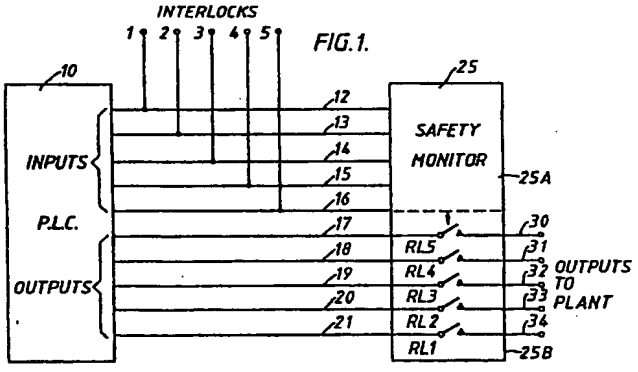


FIG.1.

EP 0 276 937 A1

each stage of the burner sequence. If there is a discrepancy, appropriate action can be initiated.

If the high air purge is less than the minimum time then power will be taken off T1 before it can time out, so the check input will not go high. The check input can be used as a clocking condition, so that if incorrect timing results, the EPROM is accessed at the wrong location, and shutdown will result.

This is illustrated in Figure 17. Here, because the check input has not gone high, the EPROM will not be stepped on. This has therefore checked the length of the purge.

The next time that can be checked is the pilot ignition time to confirm it does not exceed 5 seconds. Figure 18 shows the effect of an extended pilot ignition time. The ignition is on at the same time as the check input which means the pilot ignition period has exceeded 5 seconds.

This address can be pre-programmed as disallowed in the EPROM, and can contain a shutdown instruction. If the pilot ignition period is less than 5 seconds then the address word would be allowed, as shown in Figure 16.

The Main ignition time can be checked on timer T3 as seen from Figure 16. This timer is energised when the main valve output is energised and will then time out after 5 seconds, by which time the pilot should have been extinguished. However, if the pilot stays on for longer than 5 seconds, then when timer T3 times out, the pilot output will still be energised. This is shown in Figure 19. This can be pre-programmed as a disallowed address and so contain a shutdown instruction.

This configuration has thus checked the purge time, pilot ignition time and the Main ignition time.

The timers can be configured by standard preset solid state timers. If any timer should fail then any error will be picked up by the check input of the EPROM address line and appropriate action instigated.

The EPROM used in the monitor system can be pre-programmed with data at its various locations using standard techniques or by the use of a short program.

Claims

1. A monitor system for monitoring a microprocessor based control device in safety critical situations, said system including :-
first input means for receiving control information from the microprocessor based control device;
second input means for receiving reference information also received by said control device;
means for determining whether the control information from said device corresponds to that expected in view of the reference information, and means for overriding the control information if any error in this control information is detected.

2. A system as claimed in claim, wherein the determining means includes a memory for storing binary data accessable in dependence on information received from the first and second input means.

3. A system as claimed in claim 2, wherein the memory comprises a ROM for receiving information derived from the control device and said reference information so as to address locations therein.

4. A system as claimed in claim 2 or 3, wherein the memory is configured to contain information mirroring the control device information and to contain overriding information, the information mirroring the control device information being located at addresses accessible during normal operation of the control device and the overriding information being located at addresses accessible during an error phase of the control device.

5. A system as claimed in claim 4, including selector means, and wherein the memory has sufficient capacity to store additional sequencing information for receipt by the selector means to cause different memory areas to be made available to the control device information and reference information.

6. A system as claimed in claim 5, wherein the selector means includes a counter, and wherein feedback means are provided from the data bus of said memory to reset or increment the counter in dependence on preprogrammable instructions within selected memory storage locations.

7. A system as claimed in any of one of claims 2 to 6, wherein the first and second input means include opto-isolators for electrically isolating the inputs and including buffers for converting the inputs to a level suitable for the address bus of the memory.

8. A system as claimed in any one of claims 2 to 7, wherein the second input means are configured to receive thermostat, air status input and flame presence information from a burner device.

9. A system as claimed in any one of claims 2 to 8, wherein the first input means is configured to receive fan, ignition, pilot, main, nd alarm information from the control device for burner control.

10. A system as claimed in any one of claims 1 to 9, including checking means provided to ensure the integrity of the monitor system is maintained.

11. A system as claimed in claim 10, wherein the checking means include a dynamically operable check circuit for continually checking system integrity.

12. A system as claimed in claim 11, including a controllable oscillator for dynamically exercising the parity of the check circuit and a lockout device for initiating operational lockout in the event of a detected failure.

13. A system as claimed in claim 12, wherein the oscillator is controlled by an output provided by the determining means.

14. A system as claimed in claim 12 or 13, including at least one relay and a relay operating circuit under the control of a signal derived from the oscillator to establish the integrity of the at least one relay.

15. A system as claimed in claim 14, wherein the at least one relay includes a bistable lockout relay having a first coil operable to a lockout condition on receipt of an error detection signal from the parity check circuit, said relay being resettable by means of a second coil.

16. A system as claimed in any preceding claim, including relay means operable in dependence on an output derived from the determining means to interrupt the passage of control information from the control device to a remote location.

17. A system as claimed in claim 16, wherein the relay means are operable to by-pass the monitor in the event of monitor failure.

18. A system as claimed in any preceding claim, including timer means operable to provide reference sequencing information for use by the determining means.

19. A monitor system for monitoring a microprocessor based control device substantially as described herein with reference to the accompanying drawings.

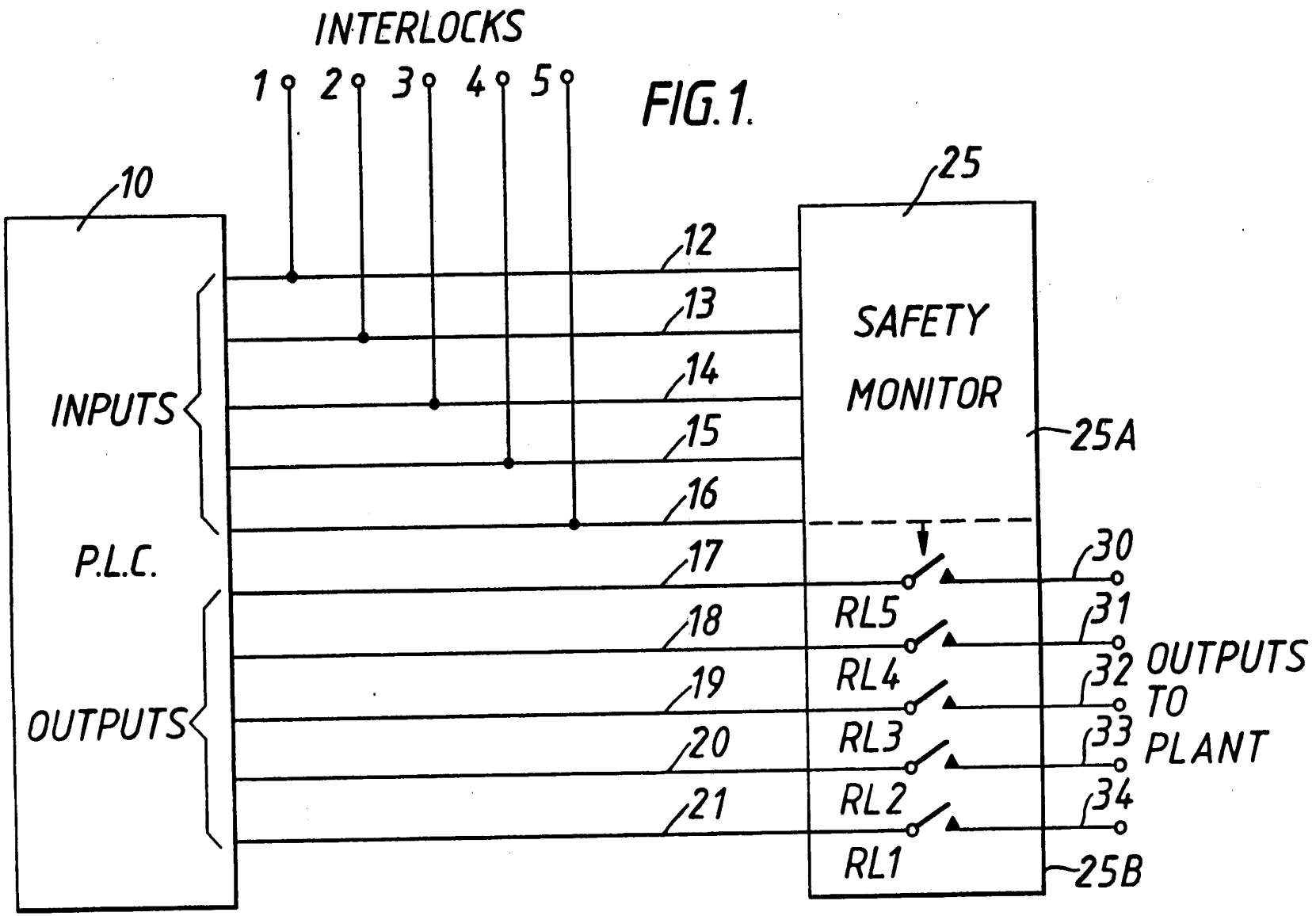

INTERLOCKS
1
2
3
4
5
10
25
12
13
14
15
16
17
18
19
20
21
INPUTS
P.L.C.
OUTPUTS
SAFETY
MONITOR
25A
RL5
RL4
RL3
RL2
RL1
25B
30
31
32
33
34
OUTPUTS
TO
PLANT

FIG.1.

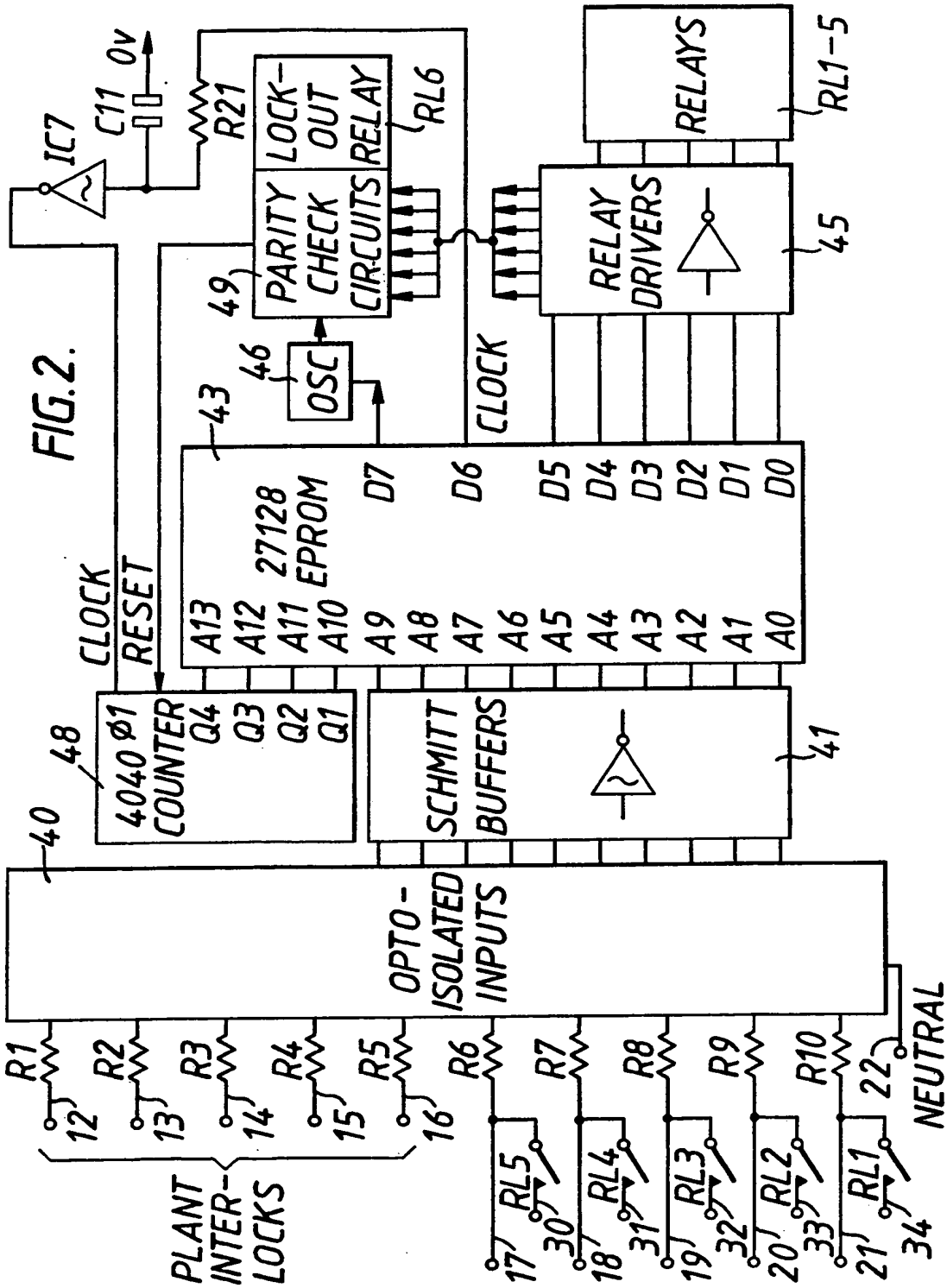


FIG.2.
IC7
C11
0v
R21
LOCK-OUT RELAY
RL6
PARITY CHECK CIRCUITS
49
46
OSC
43
27128 EPROM
A13 A12 A11 A10 A9 A8 A7 A6 A5 A4 A3 A2 A1 A0
D7 D6 D5 D4 D3 D2 D1 D0
CLOCK
RELAY DRIVERS
45
RELAYS
RL1-5
CLOCK
RESET
48
4040 Ø1 COUNTER Q4 Q3 Q2 Q1
40
SCHMITT BUFFERS
41
OPTO-ISOLATED INPUTS
R1 R2 R3 R4 R5 R6 R7 R8 R9 R10
12 13 14 15 16 17 18 19 20 21 22
PLANT INTER-LOCKS
RL5 RL4 RL3 RL2 RL1
30 31 32 33 34
NEUTRAL

FIG.3.

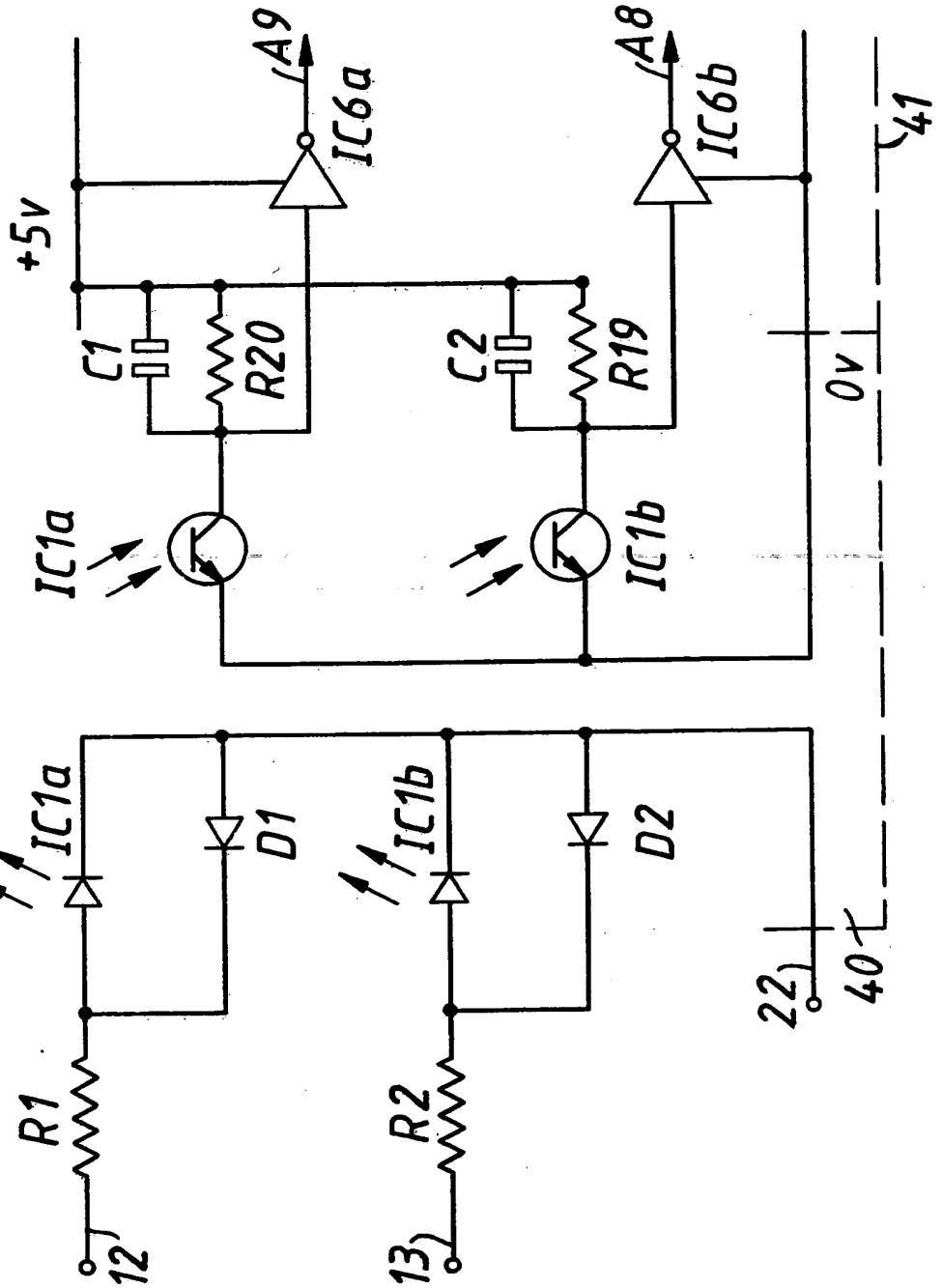

+5v
A9
IC6a
A8
IC6b
41
C1
R20
C2
R19
0v
IC1a
IC1b
IC1a
D1
IC1b
D2
R1
R2
12
13
22
40

FIG. 4.

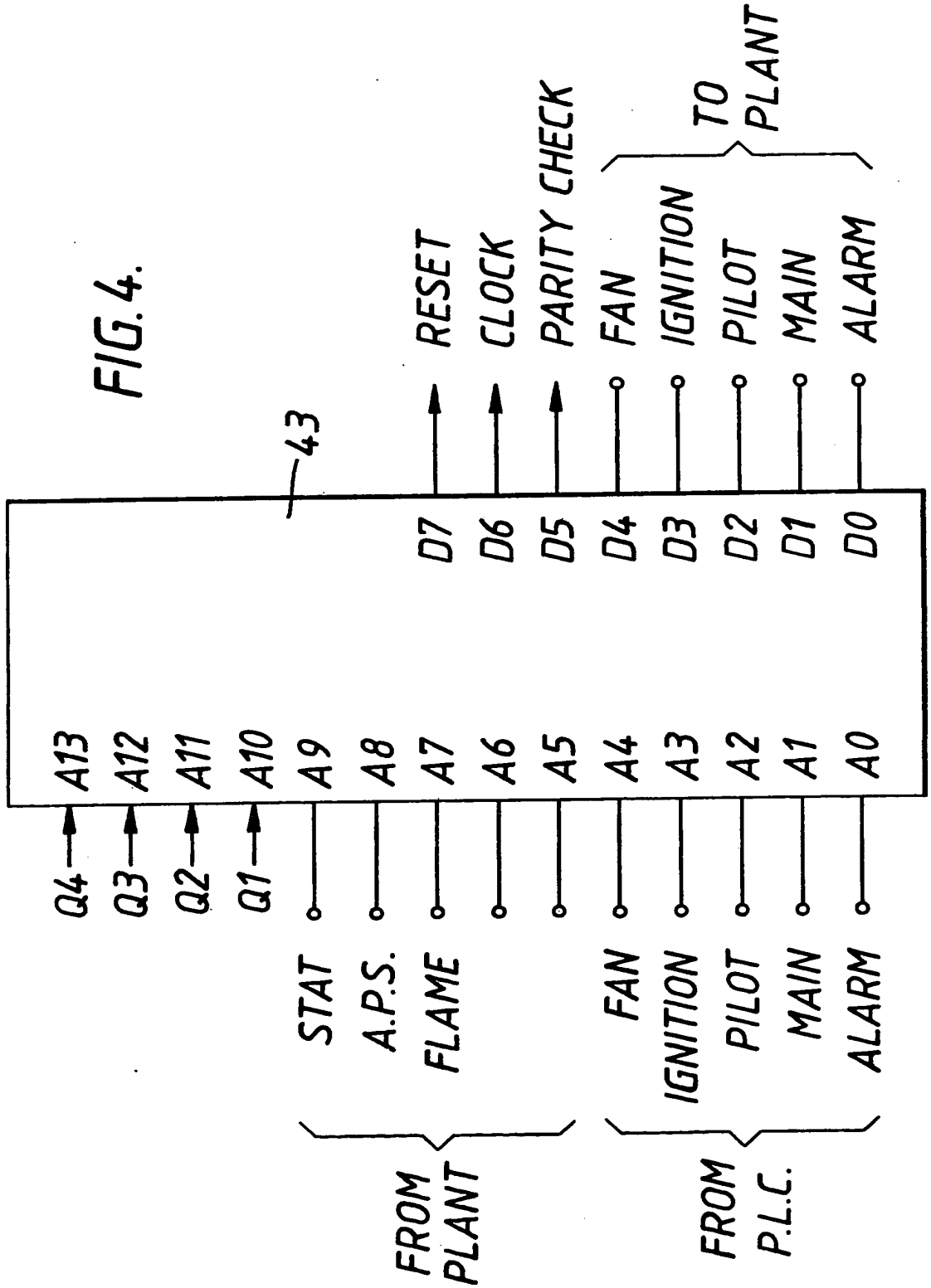

43
RESET
CLOCK
PARITY CHECK
FAN
IGNITION
PILOT
MAIN
ALARM
TO PLANT
D7
D6
D5
D4
D3
D2
D1
D0
A13
A12
A11
A10
A9
A8
A7
A6
A5
A4
A3
A2
A1
A0
Q4
Q3
Q2
Q1
STAT
A.P.S.
FLAME
FAN
IGNITION
PILOT
MAIN
ALARM
FROM PLANT
FROM P.L.C.

FIG. 5.

Stage	Period T	Main	Pilot	Ign	Fan	Flame	Alarm	APS	Stat
Shutdown	0	0	0	0	0	0	0	0	X
Start	1	0	0	0	X	0	0	0	1
Purge	2	0	0	0	1	0	0	X	1
Proven-Purge	3	0	0	X	1	0	0	1	1
Pilot-Ignition	4	0	X	1	1	X	0	1	1
Pilot-Proving	5	0	1	0	1	1	0	1	1
Main-Igninition	6	1	1	0	1	1	0	1	1
Main-Run	7	1	0	0	1	1	0	1	1
Post-Purge	8	0	0	0	1	X	0	X	0

0 = Output must be de-energised
1 = Output must be energised
X = Output - state is not critical (don't care)

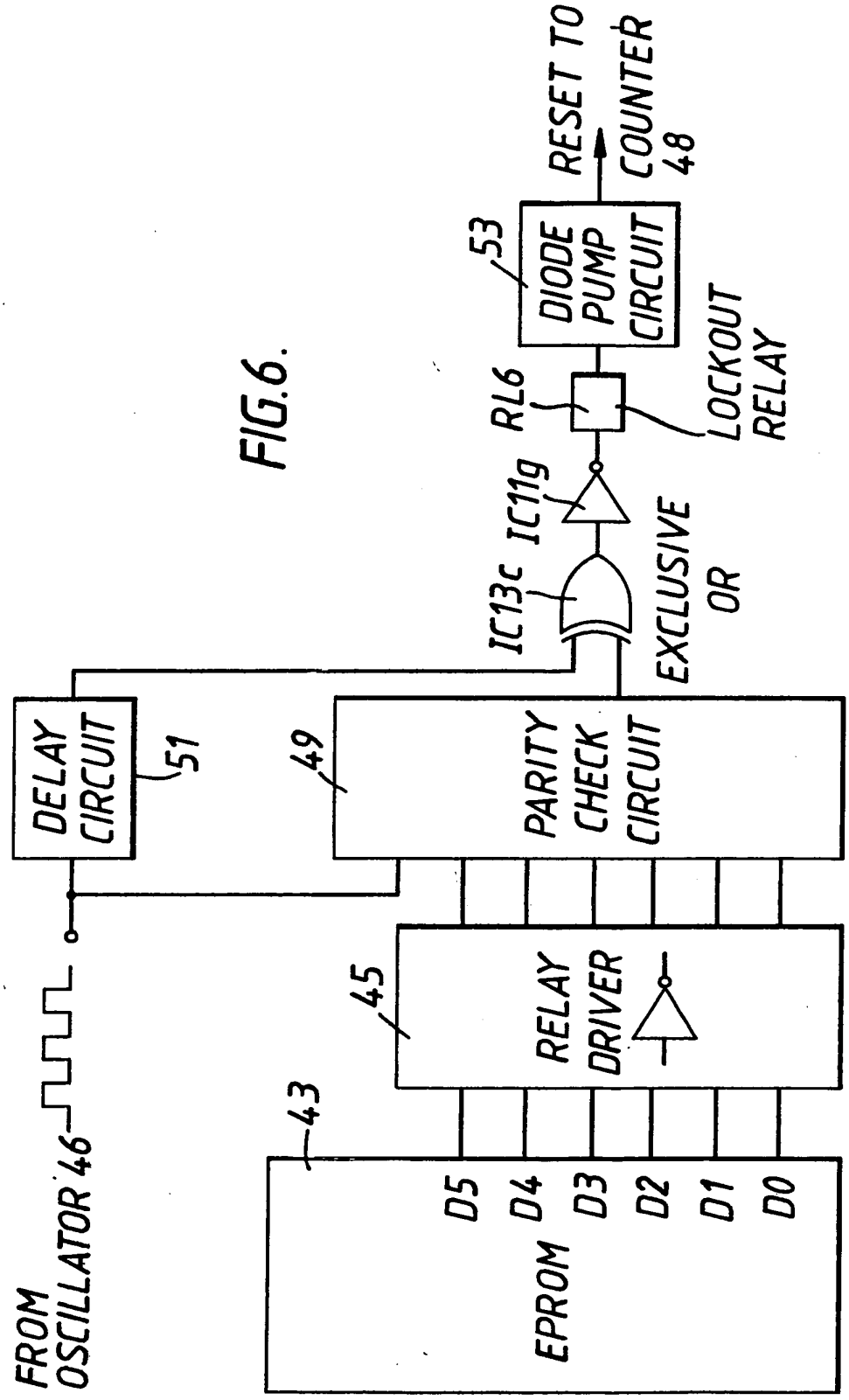
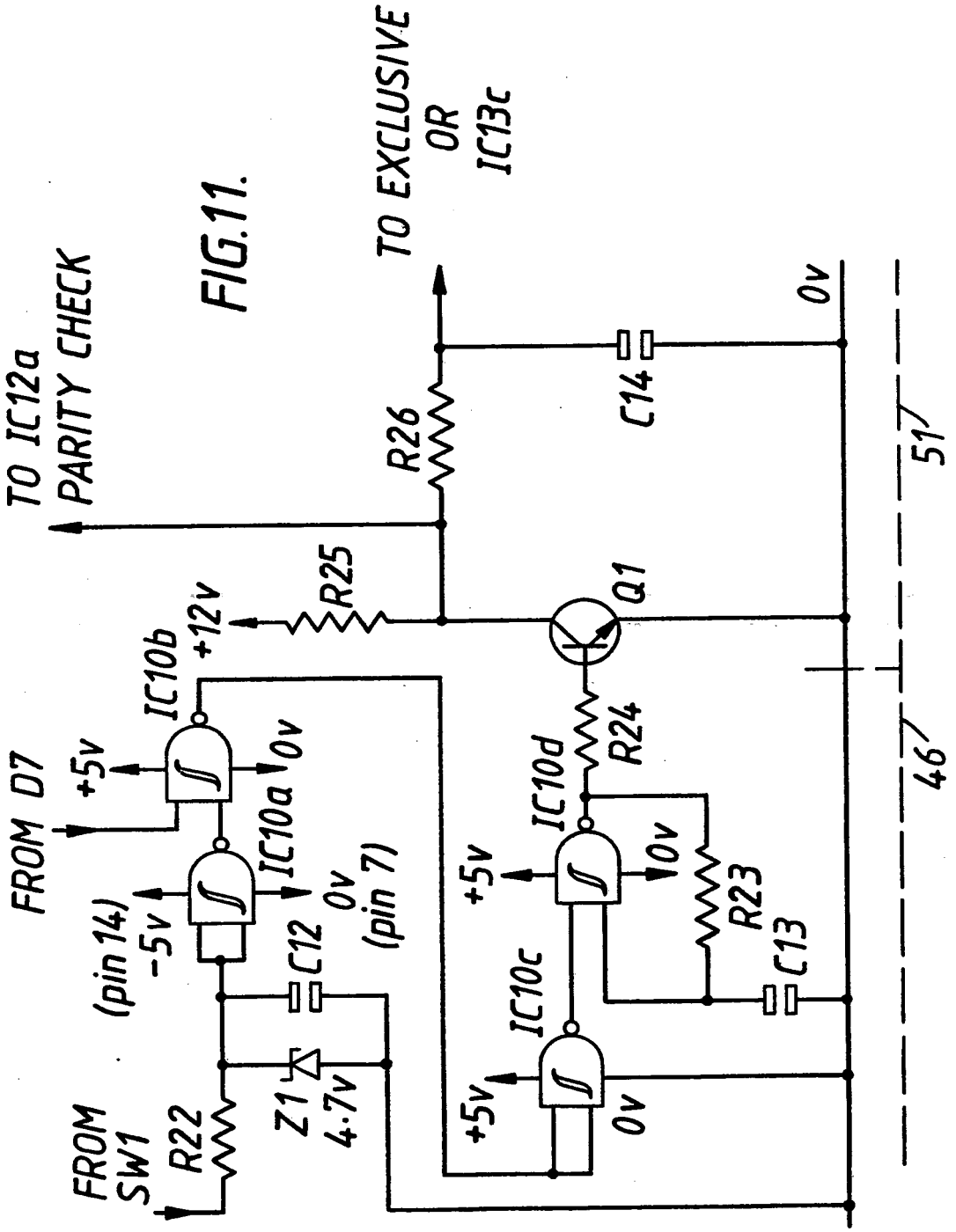

FROM OSCILLATOR 46
43
EPROM
D5
D4
D3
D2
D1
D0
45
RELAY DRIVER
49
PARITY CHECK CIRCUIT
DELAY CIRCUIT
51
IC13c
IC11g
EXCLUSIVE OR
RL6
LOCKOUT RELAY
53
DIODE PUMP CIRCUIT
RESET TO COUNTER 48

FIG.6.

FIG.11.


TO IC12a
PARITY CHECK
TO EXCLUSIVE
OR
IC13c
FROM D7
FROM
SW1
(pin 14)
-5v
+5v
+12v
0v
IC10a
IC10b
IC10c
IC10d
R22
R23
R24
R25
R26
C12
C13
C14
Z1
4·7v
Q1
0v
(pin 7)
51
46

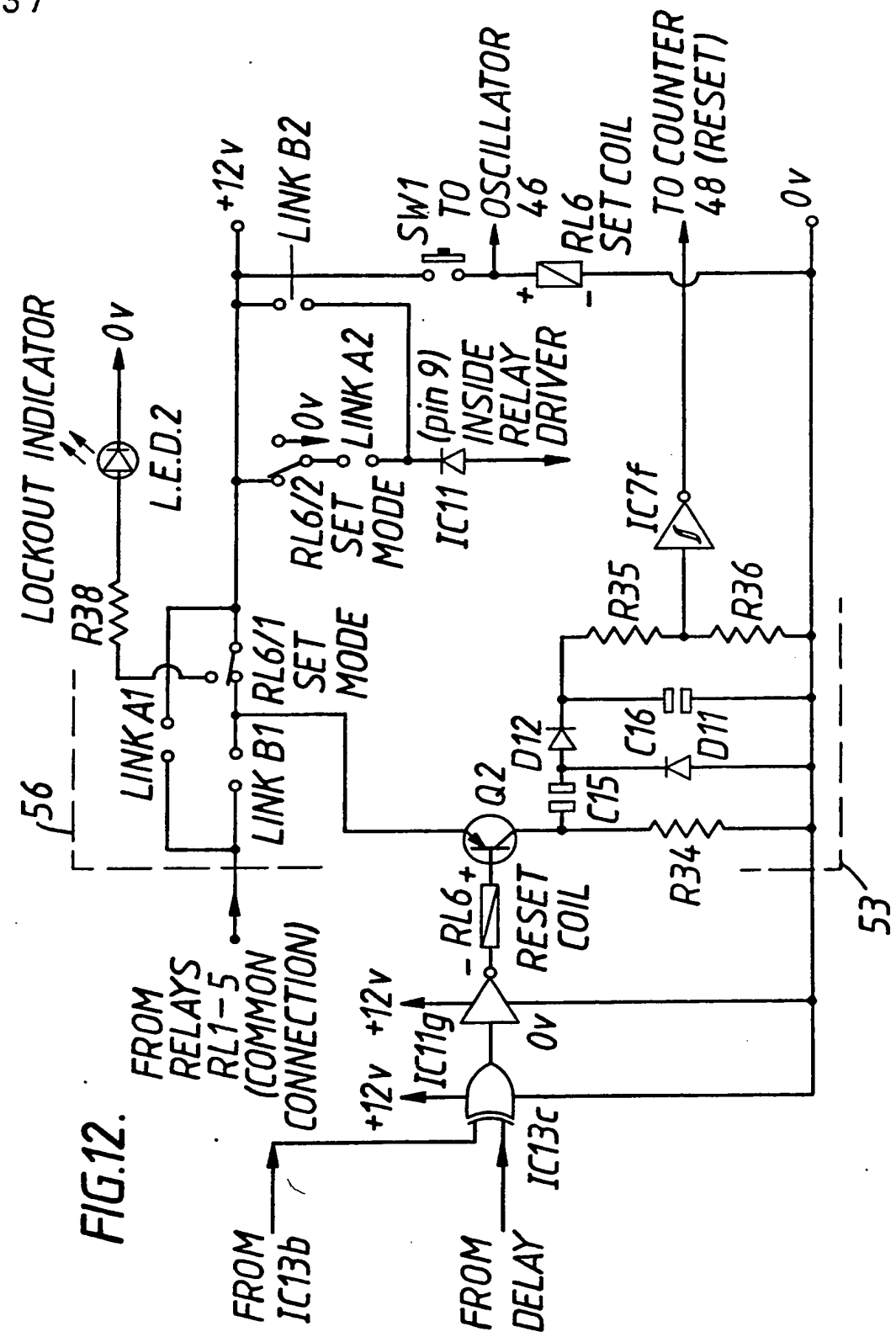

FROM IC13b
FROM DELAY
IC13c
+12v
IC11g
+12v
0v
FROM RELAYS RL1-5 (COMMON CONNECTION)
RL6 RESET COIL
Q2
D12
C15
C16
D11
R34
R35
R36
IC7f
TO COUNTER 48 (RESET)
RL6 SET COIL
SW1 TO OSCILLATOR 46
+12v
LINK B2
IC11 (pin 9) INSIDE RELAY DRIVER
RL6/2 SET MODE
0v
LINK A2
RL6/1 SET MODE
LINK A1
LINK B1
R38
LOCKOUT INDICATOR
L.E.D.2
0v
56
53

FIG.12.

FIG.13.

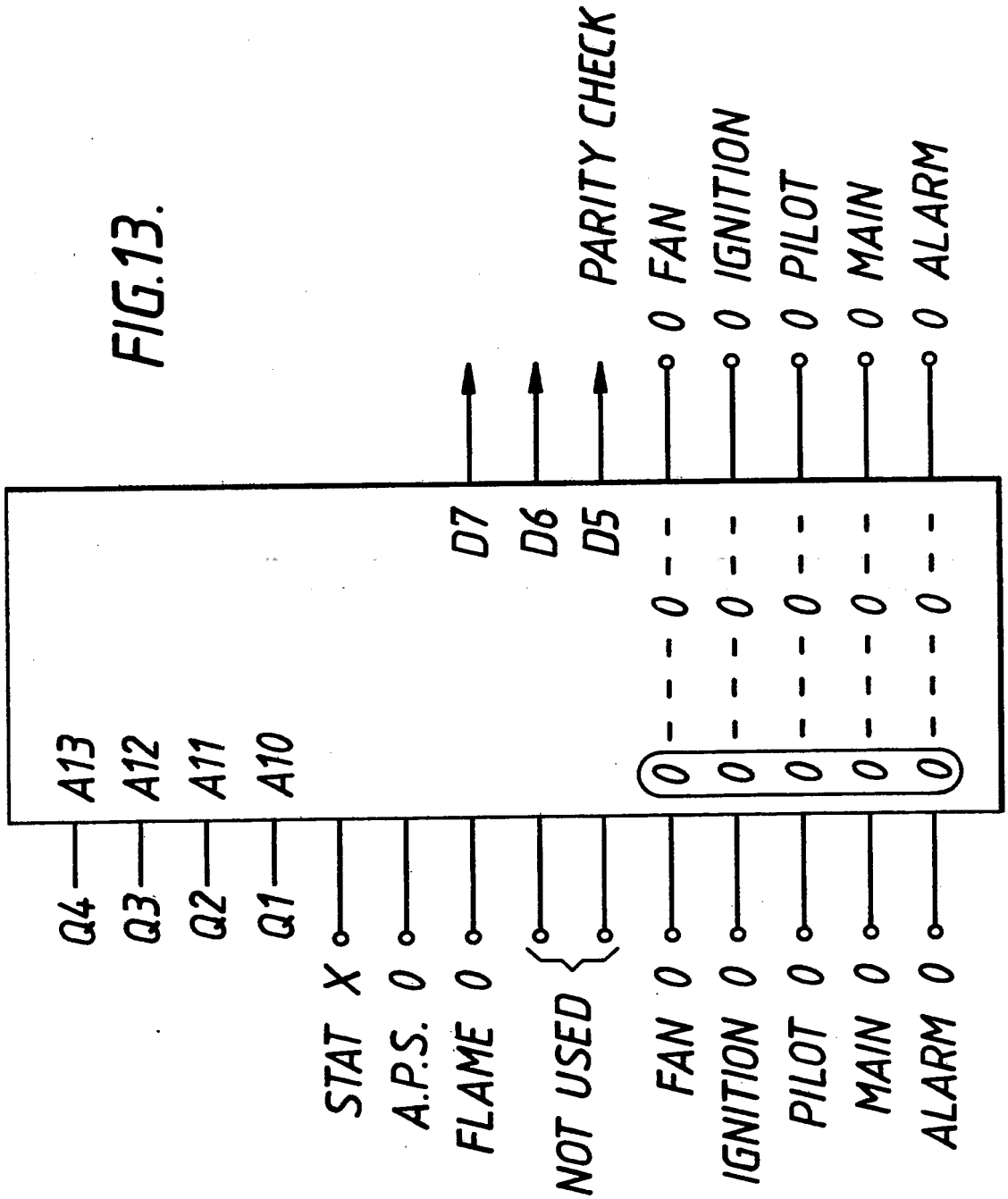

A13
A12
A11
A10
D7
D6
D5
PARITY CHECK
0 FAN
0 IGNITION
0 PILOT
0 MAIN
0 ALARM
Q4
Q3
Q2
Q1
STAT X
A.P.S. 0
FLAME 0
NOT USED
FAN 0
IGNITION 0
PILOT 0
MAIN 0
ALARM 0

FIG.14.

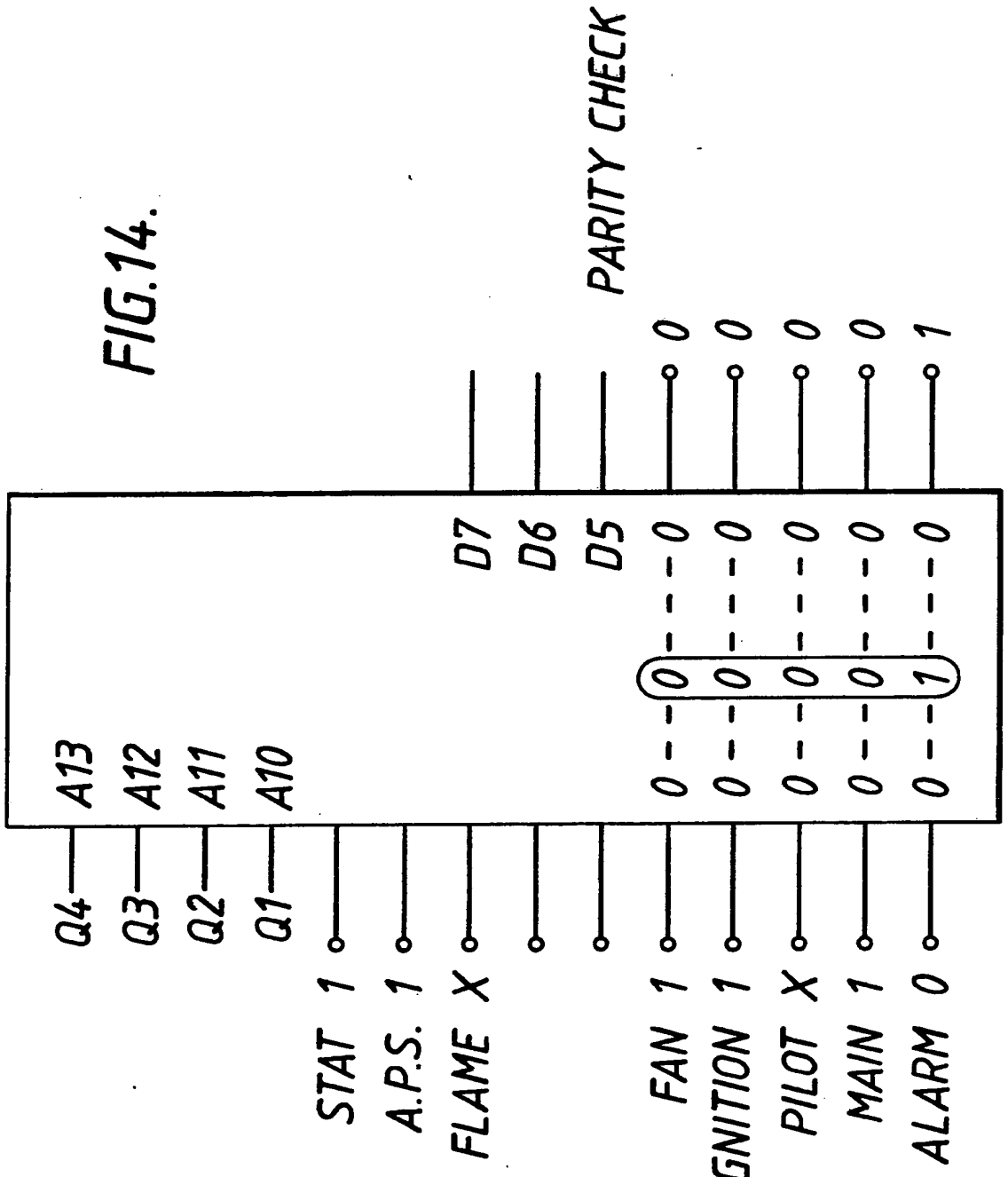

PARITY CHECK
D7
D6
D5
A13
A12
A11
A10
Q4
Q3
Q2
Q1
STAT 1
A.P.S. 1
FLAME X
FAN 1
IGNITION 1
PILOT X
MAIN 1
ALARM 0
0 0 0 0 1
0 0 0 0 0
0 0 0 0 0
0 0 0 0 0
0 0 0 0 0
0 0 0 0 1

FIG.15.

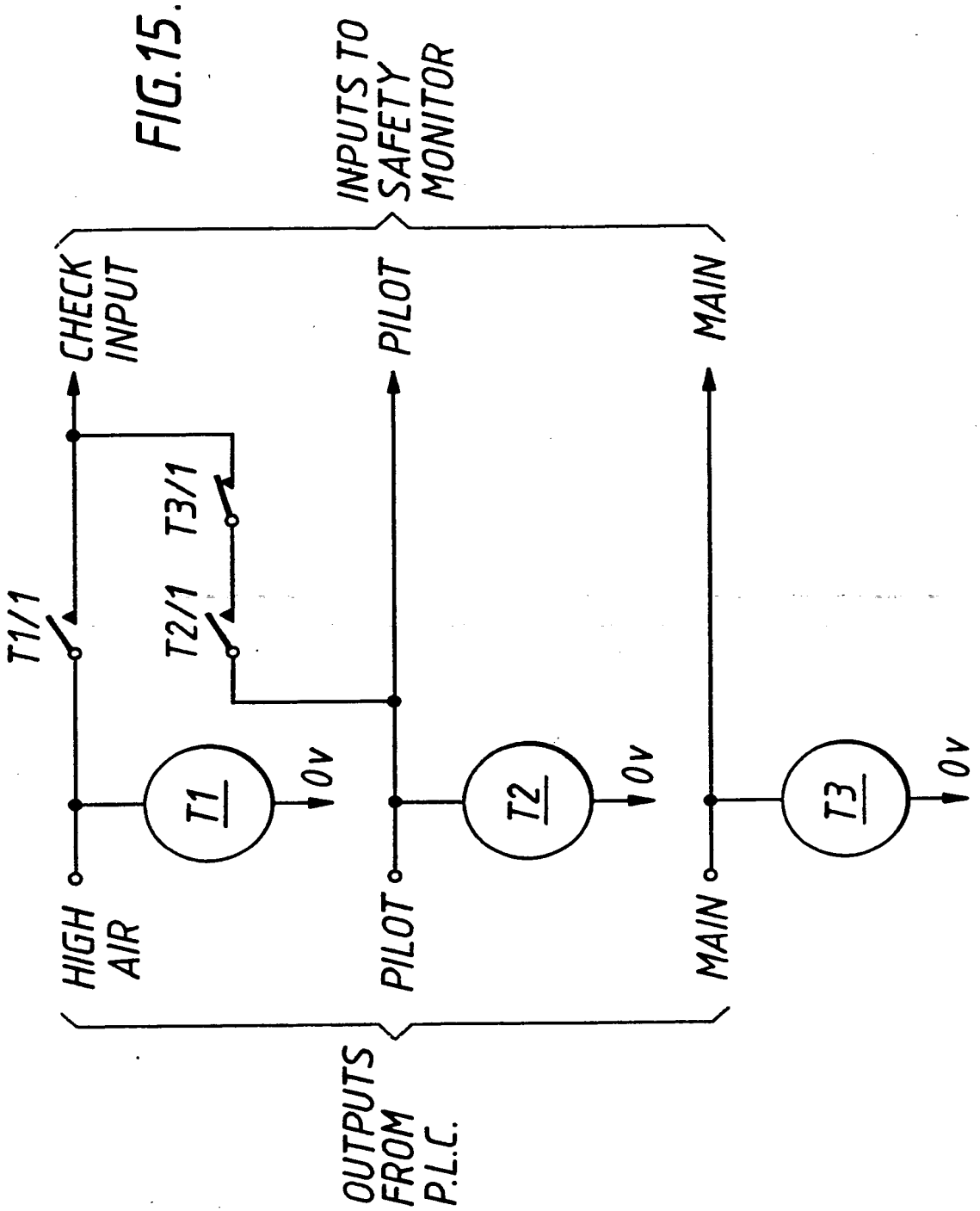

INPUTS TO SAFETY MONITOR
CHECK INPUT
PILOT
MAIN
T1/1
T2/1
T3/1
T1
T2
T3
0v
0v
0v
HIGH AIR
PILOT
MAIN
OUTPUTS FROM P.L.C.

FIG.16.

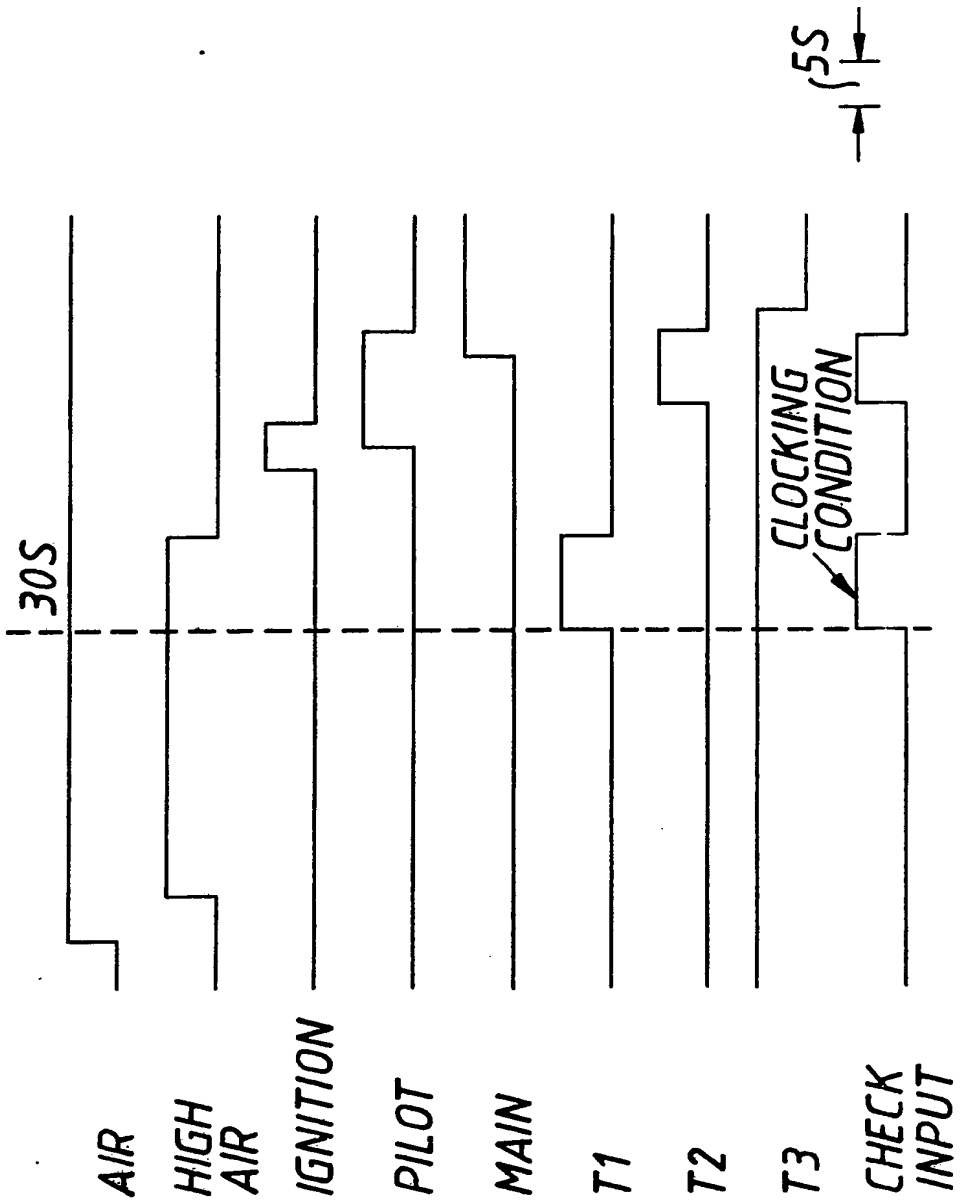

5S
30S
CLOCKING CONDITION
AIR
HIGH AIR
IGNITION
PILOT
MAIN
T1
T2
T3
CHECK INPUT

FIG.17.

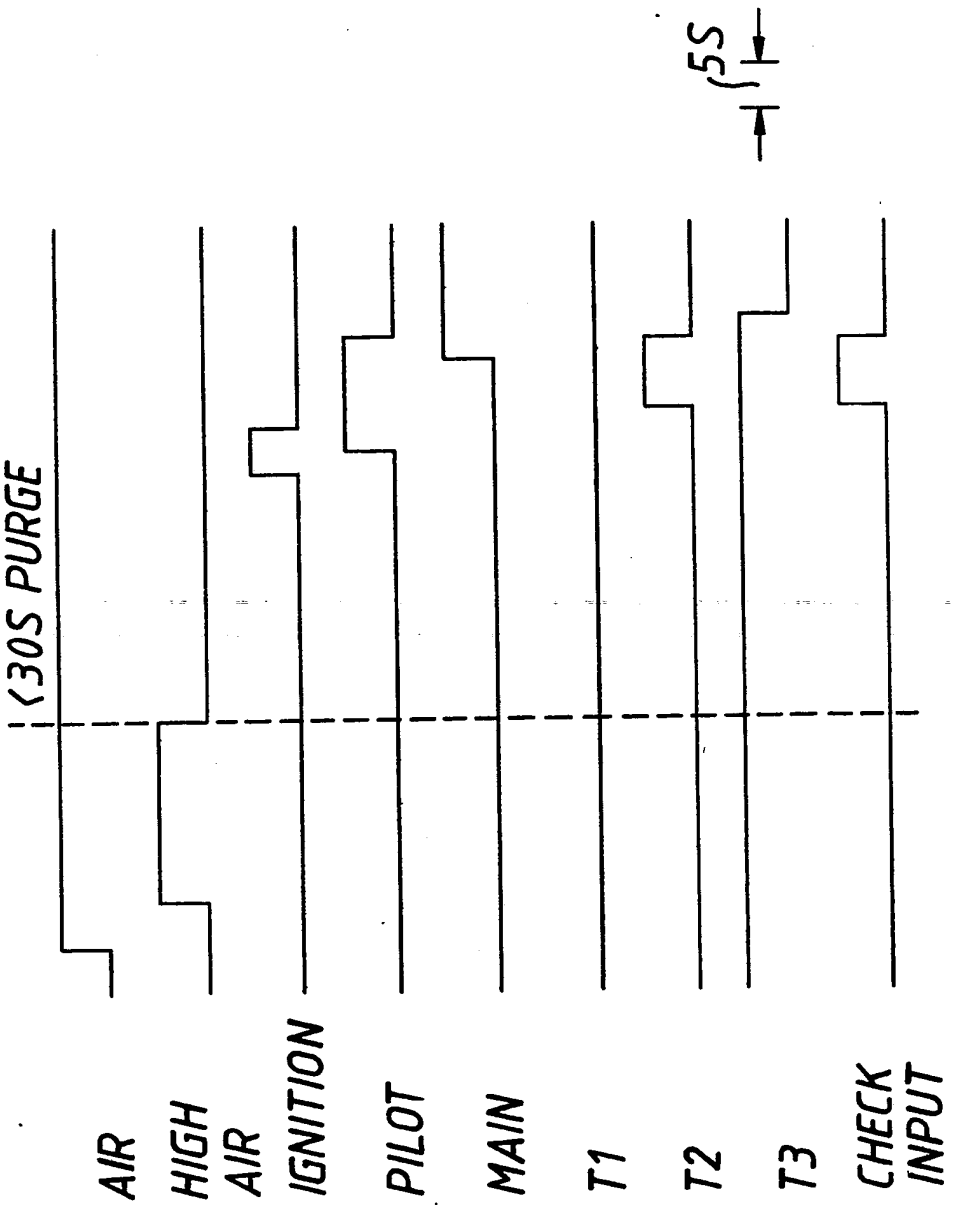
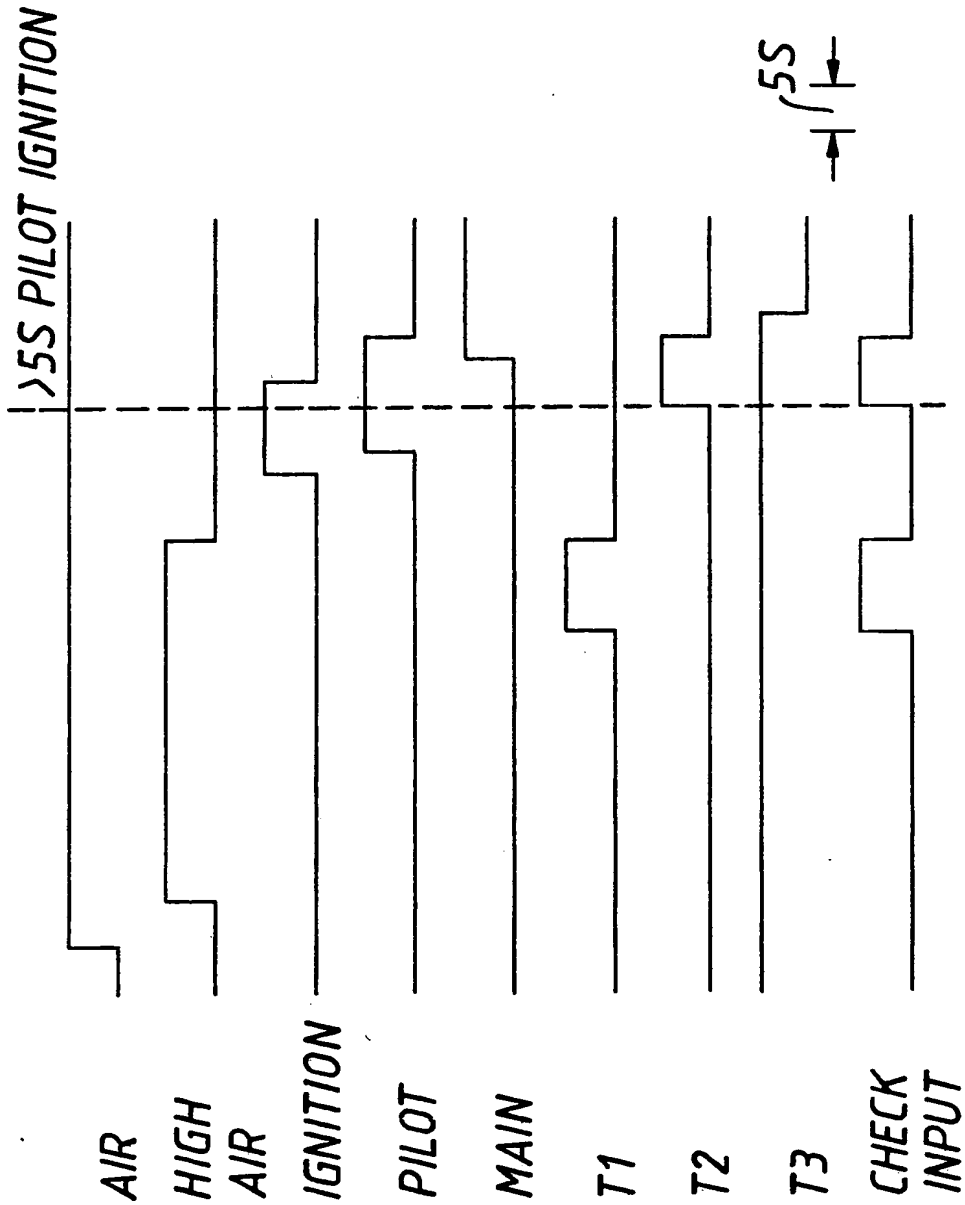

5S
30S PURGE
AIR
HIGH AIR
IGNITION
PILOT
MAIN
T1
T2
T3
CHECK INPUT

FIG.18.


>5S PILOT IGNITION
5S
AIR
HIGH AIR
IGNITION
PILOT
MAIN
T1
T2
T3
CHECK INPUT

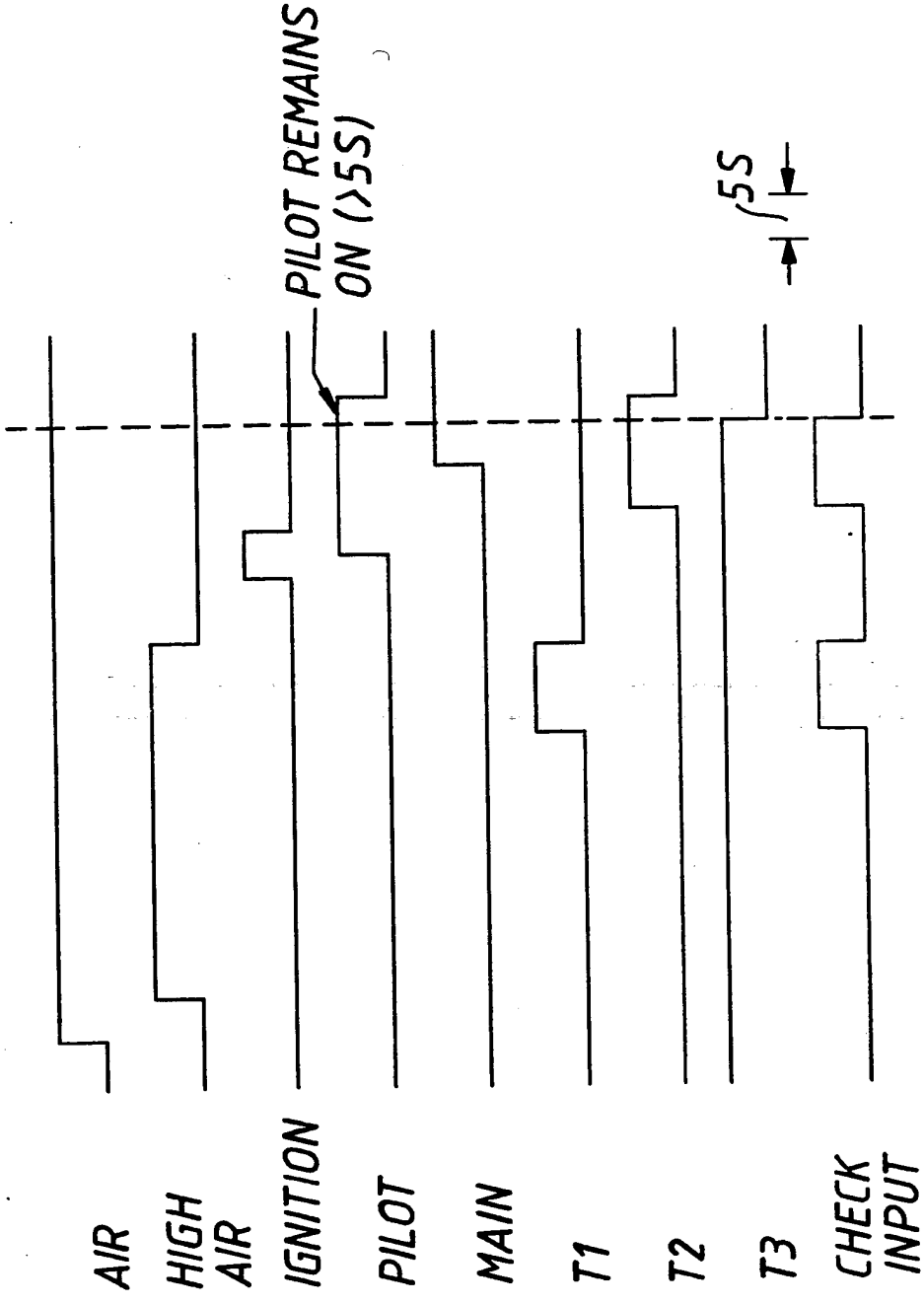

PILOT REMAINS ON (>5S)
5S
AIR
HIGH AIR
IGNITION
PILOT
MAIN
T1
T2
T3
CHECK INPUT

FIG.19.

European Patent Office

EUROPEAN SEARCH REPORT

Application Number

EP 88 30 0375

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl.4)
Y	EP-A-0 155 213 (MERLIN GERIN) * Page 2, line 8 - page 3, line 11; page 6, lines 17-36; page 7, lines 13-27; page 9, line 33 - page 10, line 10; page 10, line 29 - page 13, line 12; figures 2,3 *	1-3,7, 10-12, 16-19	G 05 B 19/04
Y	US-A-4 117 317 (DOOLEY) * Column 3, lines 48-50; column 4, lines 7-23,32-44,53-66; figures 1,2 *	1-3,7, 19	
Y	EP-A-0 155 994 (JEUMONT-SCHNEIDER) * Page 1, line 29 - page 2, line 5; page 2, lines 21-29; page 4, lines 13-29; page 5, lines 8-13,22-25; figure 1 *	10	
Y	US-A-3 701 113 (DIGITAL EQUIPMENT) * Column 2, line 48 - column 3, line 8; column 4, line 63 - column 5, line 15; column 5, line 30 - column 6, line 15; column 9, lines 3-15; column 11, line 53 - column 12, line 5; figure 1 *	11,12, 18	TECHNICAL FIELDS SEARCHED (Int. Cl.4) G 05 B 19/00
Y	FR-A-2 258 660 (ALLEN-BRADLEY) * Page 15, line 38 - page 16, line 23; figure 1 *	16,17	
A	FR-A-2 275 819 (WESTINGHOUSE) * Page 2, line 33 - page 4, line 4; page 6, line 16 - page 7, line 13 *	1-3,18-19	
A,D	GB-A-2 139 782 (EMERSON)		

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	28-03-1988	HAUSER L.E.R.

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P0401)